



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/676,850	09/30/2003	Nicholas M. Ryan	2222.5440000	3054
20210 7590 10/30/2007 DAVIS & BUJOLD, P.L.L.C. 112 PLEASANT STREET CONCORD, NH 03301			EXAMINER KLIMACH, PAULA W	
			ART UNIT 2135	PAPER NUMBER
			MAIL DATE 10/30/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/676,850

Applicant(s)

RYAN, NICHOLAS M.

Examiner

Paula W. Klimach

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 21 August 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-22 and 26-29 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-22 and 26-29 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 08/21/07. The amendment filed on 08/21/07 have been entered and made of record.

Response to Arguments

Applicant's arguments filed 08/21/07 have been fully considered.

The newly cited art, Singhal, teaches the limitations that the applicant argues are missing from the previous rejection.

The applicant pointed out that the reference, Vainstein, is disqualified as a reference. This reference has been replaced.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 6-9 and 23-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Batten-Carew et al (6,603,857 B1) in view of Singhal et al (6,851,050 B2).

In reference to claims 6, 26, and 29 Batten-Carew discloses a method and apparatus for controlling release of time-sensitive information is accomplished by a server that establishes access information for a specific future time as passed (abstract). The method includes

Art Unit: 2135

identifying an electronic document to be secured, the electronic document having at least a data portion that contains data (column 2 lines 59-67); obtaining a time-based access key (column 3 lines 24-50); securing the electronic document through use of the time-based access key to produce a secured electronic document (column 3 lines 49-52); and storing the secured electronic document (column 50-52).

Batten-Carew does not disclose determining whether a time-based access key is already available for a predetermined time, otherwise generating a time-based key for the predetermined time.

Singhal discloses a method, system, and computer program for a secure access techniques to provide user-centric authentication and allow policy-driven packet filtering (abstract). The method a system include determining whether a time-based access key (session key) is already available for a predetermined time, otherwise generating a time-based key for the predetermined time (column 18 lines 30-60).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to create a key when there is no time-based key (session key) as in the system of Singhal in the system of Batten-Crew. One of ordinary skill in the art would have been motivated to do this because when only one session key is created for a client server connection, the session key may be used to represent the particular connection.

In reference to claims 7 and 27, Batten-Carew discloses a method wherein the time-based access key has an access time associated therewith (column 3 lines 4-23).

In reference to claims 8 and 28 Batten-Carew discloses a method wherein said method further comprises: storing the time-based access key at a remote key store, and wherein the

Art Unit: 2135

time-based access key is subsequently retrievable from the remote key store only if the current time equals or exceeds the access time associated with the time-based access key (Fig. 1 and Fig. 3).

In reference to claim 9 Batten-Carew discloses a method wherein said method is performed on a client machine that operatively receives the time-based access key from the remote key store over a network (Fig. 1 and column 3 lines 32-35).

Claims 10-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Batten-Carew in view of Evans (2002/0099947 A1) and further in view of Singhal.

In reference to claim 10 Batten-Carew discloses a method and apparatus for controlling release of time-sensitive information is accomplished by a server that establishes access information for a specific future time as passed (abstract). The method comprising: identifying an electronic document to be secured, the electronic document having at least a data portion that contains data (column 2 lines 59-67); obtaining a document key (column 3 lines 30-35); obtaining a time-based access key (column 3 lines 34-39); forming a secured electronic document from at least the encrypted data portion and the encrypted document key (column 3 lines 49-52); and storing the secured electronic document (column 3 lines 50-52).

Although Batten-Crew discloses obtaining a time-based key, Batten-Carew does not disclose encrypting the data portion of the electronic document using the document key to produce an encrypted data portion; encrypting the document key using the time-based access key to produce an encrypted document key.

Art Unit: 2135

Evans discloses encrypting the data portion of the electronic document using the document key to produce an encrypted data portion (paragraph 0025)

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to encrypt the data portion of the electronic document using the document key as in Evans using the time-based access key of Batten-Crew. One of ordinary skill in the art would have been motivated to do this because the data would be stored as an encrypted document and this would ensure the content would be protected (Evans paragraph 0022).

Batten-Carew does not disclose determining whether a time-based access key is already available for a predetermined time, otherwise generating a time-based key for the predetermined time.

Singhal discloses a method, system, and computer program for a secure access techniques to provide user-centric authentication and allow policy-driven packet filtering (abstract). The method a system include determining whether a time-based access key (session key) is already available for a predetermined time, otherwise generating a time-based key for the predetermined time (column 18 lines 30-60).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to create a key when there is no time-based key (session key) as in the system of Singhal in the system of Batten-Crew. One of ordinary skill in the art would have been motivated to do this because when only one session key is created for a client server connection, the session key may be used to represent the particular connection.

In reference to claim 11 Batten-Carew discloses a method wherein the time-based access key is a public time-based access key (column 4 lines 56-65).

In reference to claim 12 Batten-Carew discloses a method wherein the time-based access key has an access time associated therewith (Fig. 2).

In reference to claim 13 Batten-Carew discloses a method wherein the time-based access key is available from a remote key store only if the current time equals or exceeds the access time associated with the time-based access key (Fig. 3).

In reference to claim 14 Batten-Carew discloses a method wherein the access time is a day of a year, and the time-based access keys are unique for each day of the year (Fig. 2).

In reference to claim 15 Batten-Carew discloses a method wherein said method is performed on a client machine that operatively receives the time-based access key from the remote key store over a network (Fig. 1 and column 3 lines 32-35).

Claims 16-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Evans in view of Batten-Carew.

In reference to claim 16 Mulder discloses a method for secure electronic information exchange between a sender and a recipient (abstract). The system performs a method that includes obtaining an encrypted document key from the header portion of the secured electronic document (paragraph 0025); decrypting an encrypted data portion of the secured electronic document using the document key to produce a data portion (paragraph 0025); and supplying the data portion to the requester (paragraph 0026).

Evans does not disclose obtaining a time-based access key and decrypting the encrypted document key using the time-based access key to produce a document key.

Batten-Carew discloses a method and apparatus for controlling release of time-sensitive information is accomplished by a server that establishes access information for a specific future time as passed (abstract). The method of Batten-Carew includes obtaining a time-based access key (Fig. 3) and decrypting the encrypted document key using the time-based access key to produce a document key (column 4 lines 57-65).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the time-based key of Batten-Carew in the system of Evans. One of ordinary skill in the art would have been motivated to do this because the method of Batten-Carew would allow time-sensitive information to be released at any time and accessed only at a specific future time based on the release of access information relating to the specific future time (column 2 lines 29-33).

In reference to claim 17 Evans discloses a method wherein the time-based access key (document keys) is identified by an indicator within a header portion of the secured electronic document (Fig. 2).

In reference to claim 18 Evans does not discloses a method wherein the time-based access key is a private time-based access key

Batten-Carew discloses a method wherein the time-based access key is a private time-based access key (column 3 lines 57-64).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the time-based key of Batten-Carew in the system of Evans. One of ordinary skill in the art would have been motivated to do this because the method of Batten-Carew would allow time-sensitive information to be released at any time and accessed only at a

Art Unit: 2135

specific future time based on the release of access information relating to the specific future time (column 2 lines 29-33).

In reference to claim 19 Evans does not disclose a method wherein the time-based access key being obtained is acquired from a server.

Batten-Carew does not disclose a method wherein the time-based access key being obtained is acquired from a server (Fig. 1).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the time-based key of Batten-Carew in the system of Evans. One of ordinary skill in the art would have been motivated to do this because the method of Batten-Carew would allow time-sensitive information to be released at any time and accessed only at a specific future time based on the release of access information relating to the specific future time (column 2 lines 29-33).

In reference to claim 20 Evans does not disclose a system wherein said obtaining of the time-based access key is dependent on the current time..

Batten-Carew discloses a system wherein said obtaining of the time-based access key is dependent on the current time (Fig. 3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the time-based key of Batten-Carew in the system of Evans. One of ordinary skill in the art would have been motivated to do this because the method of Batten-Carew would allow time-sensitive information to be released at any time and accessed only at a specific future time based on the release of access information relating to the specific future time (column 2 lines 29-33).

In reference to claim 21 Evans does not disclose a system wherein the time-based access key is associated with an access time, and wherein said obtaining of the time-based access key is permitted only when the current time is greater than or equal to the access time.

Batten-Carew discloses the time-based access key is associated with an access time, and wherein said obtaining of the time-based access key is permitted only when the current time is greater than or equal to the access time (Fig. 3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the time-based key of Batten-Carew in the system of Evans. One of ordinary skill in the art would have been motivated to do this because the method of Batten-Carew would allow time-sensitive information to be released at any time and accessed only at a specific future time based on the release of access information relating to the specific future time (column 2 lines 29-33).

In reference to claim 22 Evans does not disclose a system wherein, if permitted, said obtaining obtains the time-based access key being obtained from a server.

Batten-Carew discloses a method wherein, if permitted, said obtaining obtains the time-based access key being obtained from a server (Fig. 3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the time-based key of Batten-Carew in the system of Evans. One of ordinary skill in the art would have been motivated to do this because the method of Batten-Carew would allow time-sensitive information to be released at any time and accessed only at a specific future time based on the release of access information relating to the specific future time (column 2 lines 29-33).

Claims 1-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mulder et al (2002/0172367) in view of Batten-Carew.

In reference to claim 1 Mulder discloses a method for secure electronic information exchange between a sender and a recipient (abstract). The system of Mulder includes a key store (the combination of public key certificates and private key storage) that stores a plurality of cryptographic key pairs, each of the cryptographic key pairs includes a public key and a private key (paragraph 0022); and an access manager (registration authority) operatively connected to said key store (paragraph 0022), said access manager determines whether the private key of the at least one of the cryptographic key pairs is permitted to be provided to a requester, the user is authenticated (paragraph 0022);

Mulder does not disclose a cryptographic key that pertains to a predetermined time.

Batten-Carew discloses a method and apparatus for controlling release of time-sensitive information is accomplished by a server that establishes access information for a specific future time as passed (abstract). The method includes at least one of the cryptographic key pairs pertaining to a predetermined time (column 3 lines 40-47); key pairs pertaining to the predetermined time is permitted to be provided to a requester based on a current time (Fig. 3), wherein the requester requires the private key of the at least one of the cryptographic key pairs pertaining to the predetermined time to access a secured electronic file (column 3 lines 48-55), and wherein the secured electronic file was previously secured using the public key of the at least one of the cryptographic key pairs pertaining to the predetermined time (Fig. 1).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the time-based key of Batten-Carew in the system of Mulder. One of ordinary skill in the art would have been motivated to do this because the method of Batten-Carew would allow time-sensitive information to be released at any time and accessed only at a specific future time based on the release of access information relating to the specific future time (column 2 lines 29-33).

In reference to claim 2 Mulder does not teach an access manager only provides the private key of the at least one of the cryptographic key pairs pertaining to the predetermined time to the requester if the predetermined time is greater than or equal to the current time.

Batten-Carew discloses a system, wherein said access manager only provides the private key of the at least one of the cryptographic key pairs pertaining to the predetermined time to the requester if the predetermined time is greater than or equal to the current time (Fig. 3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the time-based key of Batten-Carew in the system of Mulder. One of ordinary skill in the art would have been motivated to do this because the method of Batten-Carew would allow time-sensitive information to be released at any time and accessed only at a specific future time based on the release of access information relating to the specific future time (column 2 lines 29-33).

Art Unit: 2135

In reference to claim 3 Mulder discloses a system wherein the requestor is a client module that operatively connects to said access manager over a network (paragraph 0025). A user receives email on a client device.

In reference to claim 4 Mulder does not disclose a system wherein said document security system further comprises: at least one client module, said client module assists a user in selecting the predetermined time, and said client module secures the electronic file using the public key of the at least one of the cryptographic key pairs pertaining to the predetermined time so as to provide a time-based access restriction to the electronic file.

Batten-Carew discloses a system wherein said document security system further comprises: at least one client module, said client module assists a user in selecting the predetermined time, and said client module secures the electronic file using the public key of the at least one of the cryptographic key pairs pertaining to the predetermined time so as to provide a time-based access restriction to the electronic file (Fig. 4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the time-based key of Batten-Carew in the system of Mulder. One of ordinary skill in the art would have been motivated to do this because the method of Batten-Carew would allow time-sensitive information to be released at any time and accessed only at a specific future time based on the release of access information relating to the specific future time (column 2 lines 29-33).

In reference of claim 5 Mulder does not disclose a cryptographic key that pertains to a predetermined time.

Art Unit: 2135

Batten-Carew discloses a system wherein said client module further assists in unsecuring the secured electronic file by acquiring the private key of the at least one of the cryptographic key pairs that pertaining to the predetermined time from said key store, and then unsecuring the secured electronic file using the private key of the at least one of the cryptographic key pairs that pertaining to the predetermined time (Fig. 3 and Fig. 4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the time-based key of Batten-Carew in the system of Mulder. One of ordinary skill in the art would have been motivated to do this because the method of Batten-Carew would allow time-sensitive information to be released at any time and accessed only at a specific future time based on the release of access information relating to the specific future time (column 2 lines 29-33).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Time-lock Puzzle and Time-release Crypto Rivest, Shamir, Wagner 1996

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

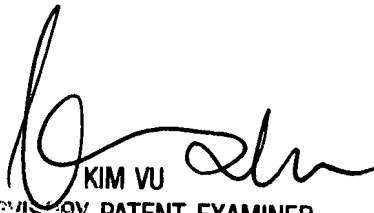
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

PWK

Saturday, October 27, 2007


KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100